ホワイトペーパー

グローバルな分散組織向けのOkta

世界最大規模の組織で「ハブアンドスポーク」モデルを活用し、セキュリティや効率を犠牲にすることなく俊敏性と柔軟性を両立

目次

グローバル組織や多様なビジネス部門でサービスを横断的に管理

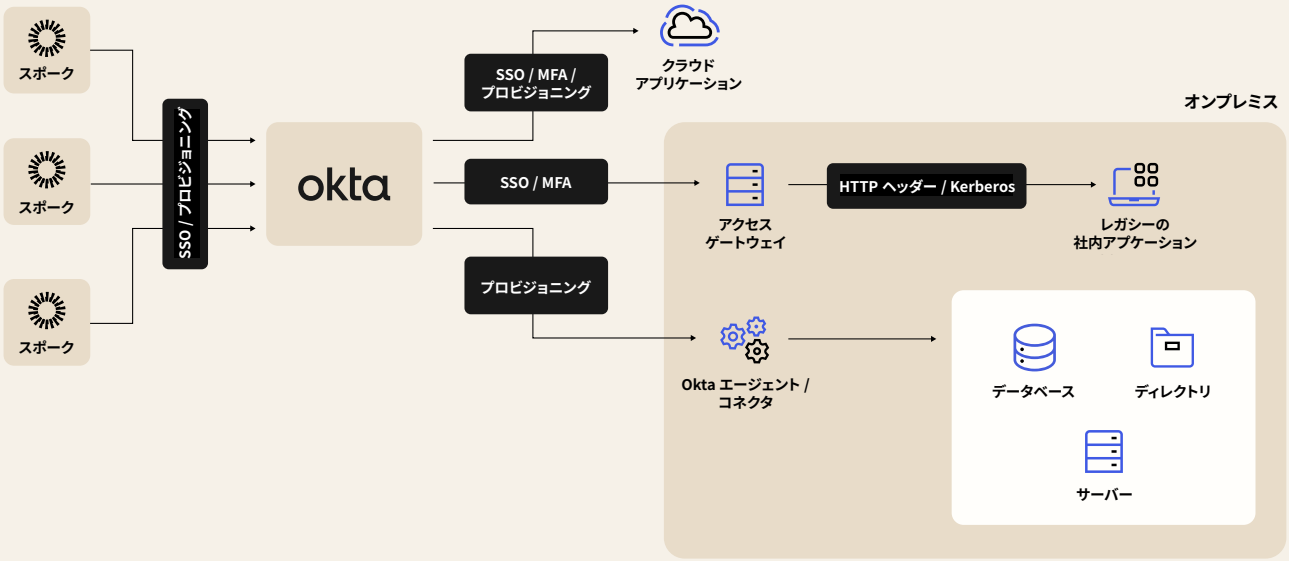
大規模で複雑な組織にとって、アイデンティティに関連するいくつもの側面を一元化することは非常に困難です。ビジネス部門、子会社、地域ごとの組織は、独立して運営していることも多く、そのような場合には独自の意思決定を行い、独自のテクノロジーやユーザーベースを管理しています。多国籍の組織は、データレジデンシーに関連する規制要件を遵守しなければならず、個人識別情報（PII）をそれぞれの国内で保管する必要があります。そのために、アイデンティティの一元化という野心的な目標は達成不可能なものに思えるかもしれません。さらに、短期的（周期的）な必要性から、あるいは M&A を含む長期の取り組みにおいて、自社の能力を強化しようとする組織は、外部から持ち込まれるアイデンティティの一元化にどのように対処すべきかという課題に直面しています。

「ハブアンドスポーク」型のアイデンティティモデルは、全社的な統合サービスや一元的な可視化の基盤となると同時に、分散する情報テクノロジー（IT）組織全体で特定のアプリケーション / ユーザー管理の柔軟性を実現します。こうしたメリットを提供するのが、Okta for Global 2000 です。ハブアンドスポークモデルを活用し、セキュリティや効率を犠牲にすることなく俊敏性と柔軟性を向上させる実際のユースケースは多数あり、以下に対応する展開モデルを利用できます。

- 複数のビジネス部門を持つ大規模組織
- データレジデンシーを持つ多国籍組織
- サードパーティ（請負業者を含む）へのアウトソーシング
- M&A 向けの統合

Okta for Global 2000 が組織の複雑性に対応

Okta のハブアンドスポーク型モデルにより、アイデンティティの集合を複数の Okta テナント（Okta org）として物理的かつ論理的に分離できます。このモデルを利用することで、通常はビジネス、技術、コンプライアンス要件といった要因に左右される複雑なユースケースにも柔軟に対応できるようになります。Okta Integration Network（OIN）の Org2Org コネクタを使用することで、複数の Okta org を統合し、シングルサインオン（SSO）とプロビジョニングの両方を数分で実現できます。



Okta のハブアンドスポーク型アーキテクチャモデル

このアーキテクチャで、ハブアンドスポークは以下のように機能します。

ハブ

1 つの Okta org がハブとなり、スポークに対して独立したサービスプロバイダー（SP）として動作し、ディレクトリサービス、認証、認可サービスの一元的な提供を担います。ハブはさらに、共通のアイデンティティ標準を使用してアイデンティティプロバイダ（IdP）として機能し、下流のアプリケーションと統合します。これにより、SSO（SAML、WS-Federation、OpenID Connect などを使用）やプロビジョニング（SCIM などを使用）の観点から、シームレスで安全なアクセスを提供します。

スポーク

1 つまたは複数の Okta org が個別のスポークとなり、ディレクトリサービス、認証、認可サービスを提供する独立した IdP として動作します。スポークのこうした責任はハブと同じですが、さらにスポーク内の各ユーザーに対して、分散管理の形でこれらの能力を提供します。スポークは、Okta の Universal Directory の独自インスタンスを利用して、ユーザープロファイル / グループ情報を保存します。Okta で直接作成された（Okta を「信頼できる唯一の情報源」とする）情報も、Active Directory、LDAP、人事情報システムその他のリポジトリをソースとする情報も、同様に対象となります。

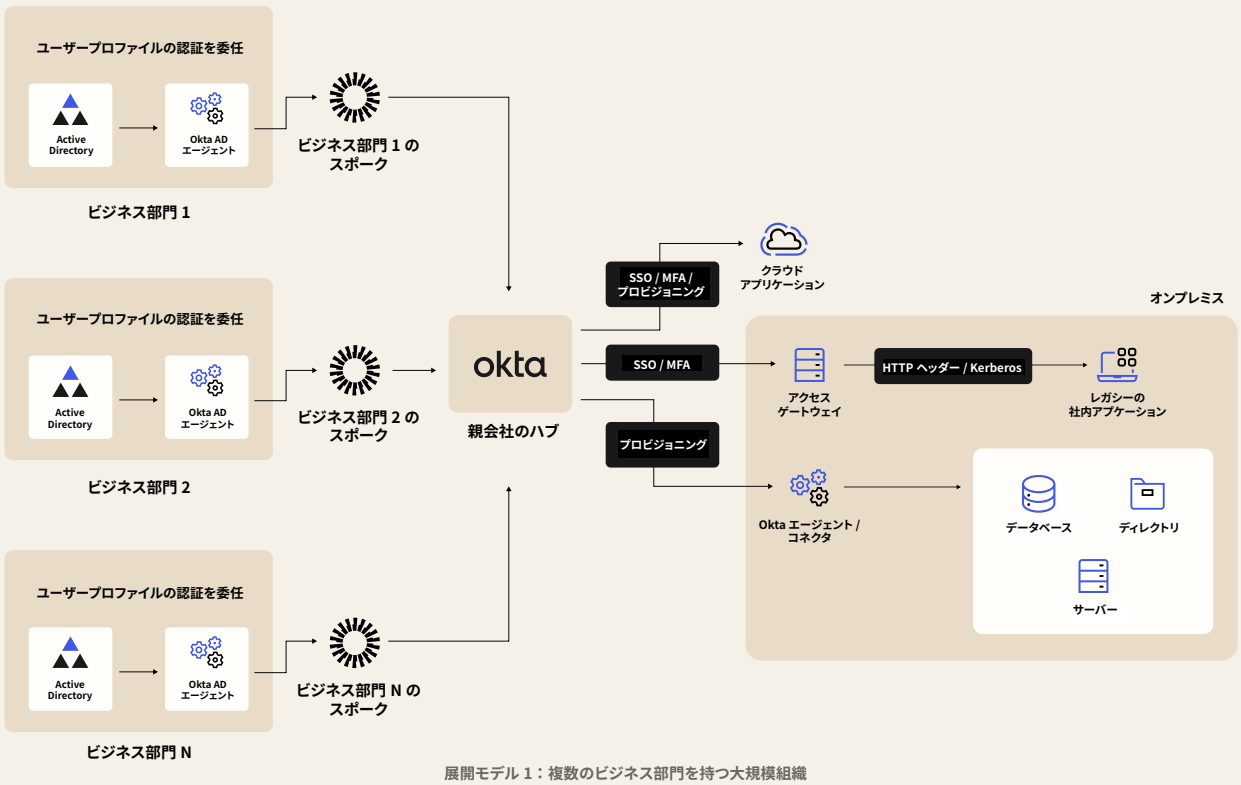
スポークは、シームレスで安全なアクセスを提供するため、Okta Integration Network（OIN）の Org2Org コネクタを活用し、ユーザープロファイルをハブにプロビジョニングして、ハブに統合されたアプリケーション / サービスへの SSO を可能します。Okta for Global 2000 は、Okta Workflows を使用し、ハブアンドスポーク型アーキテクチャ全体を自動化することで、アイデンティティ管理の複雑な課題を解決できます。社内の従業員と社外のユーザーアイデンティティの両方を管理する必要のある組織は、さまざまなシナリオでこのモデルを使用できます。

柔軟な展開モデルが俊敏性を向上

Okta for Global 2000 は、大規模組織のリーダーが柔軟性と自律性を保持しながらリソースを一元管理できるように支援することで、組織の俊敏性や効率性の向上やセキュリティの強化を可能にします。Okta の柔軟な展開モデルにより、多くのユースケースで複雑さを軽減し、俊敏性を高めることができます。

展開モデル 1：複数のビジネス部門を持つ大規模組織
大規模組織では、多数のビジネス部門が独立して管理を担っていることがあります。そうしたビジネス部門は、さまざまなテクノロジーソリューションの選定で独自の意思決定を下すことができ、IT 投資とユーザーライフサイクルの管理を部門内の担当者が受け持っている場合もあります。これらのビジネス部門の運営は独立していますが、親会社は全般的なコスト削減や全社的な効率向上のために、共有サービスモデルを通じて、すべてのビジネス部門にさまざまなテクノロジーサービスやプラットフォームを提供することがあります。このような独立したビジネス部門が、その独立性を維持しながら、さまざまなアプリケーションやプラットフォームの共有サービスモデルに参加できるようにすることは、組織的にも、テクノロジーの観点でも難しい課題となることがあります。

次に示す図は、Okta for Global 2000 をハブアンドスポーク型アーキテクチャで活用する仕組みを説明しています。このモデルで、親会社（ハブ）は、個々のビジネス部門に混乱を引き起こしたり、既存のユーザーリポジトリやテクノロジー投資に対する制御を阻害したりすることなく、オンプレミス / クラウドベースの多様なアプリケーションやプラットフォームサービスを一元化できます。各ビジネス部門は、独自に管理する既存の Active Directory ユーザーリポジトリを活用して、スポーク経由でのアプリケーションへのアクセスだけでなく、共有サービスモデルでハブが提供するアプリケーションへのアクセスも可能にします。ビジネス部門のユーザーは、ハブが提供するものを含め、すべてのアプリケーションにシームレスかつ安全に（SSO を使用して）アクセスし、Active Directory の既存の資格情報を使用して引き続き認証します。最後に、ハブは必要に応じて、下流のアプリケーションやユーザーリポジトリへのユーザーアクセスのプロビジョニングを実行できます。



展開モデル 1：複数のビジネス部門を持つ大規模組織

NTT DATA

NTT データの事例：セキュリティを強化しながらプロビジョニングを自動化

NTT にとっては、常にセキュリティが最優先事項です。同社のような大規模組織では、業務ユーザーの入社 / 離職や異動は、手作業によるプロビジョニングの負担を増やします。こうした作業は、IT リソースを消耗するだけでなく、アカウントや資格情報の孤立によってセキュリティの脆弱性を引き起こすリスクがあります。

この問題に対応するため、NTT データのハブアンドスポーク型モデルでは、14 万人以上の従業員（同姓同名の従業員も含め）の情報、ログイン、アプリを能率的に管理しています。同社は、プロビジョニングを自動化し、グループ内の各企業がつながりを保持しながら自律的に運営できるようにするため、Okta Workforce Identity Cloud を採用しました。目標の 1 つに挙げたのは、NTT ブランドのメールをすべての従業員が使用できるようにすることです。舞台裏では、中央のアイデンティティハブが 900 社以上で作成されたすべてのアイデンティティを管理し、サフィックスのブランディングによって、異なるスポーク間でアイデンティティの競合が起こらないようにしています。

Okta でプロビジョニングポイントを一元化したことで、中央のハブですべてのプロビジョニングを行った後に、各オフィスに接続できるようになりました。これにより、全組織が連携を保ちつつ、個々の事業体として活動できます。さらに、IT チームは、グラフィカルユーザーインターフェイスを簡潔化して、アプリケーション間や特定の時間枠内でカスタムのアクションをシームレスに組み合わせることにより、企業内のセキュリティと効率を向上させました。

展開モデル 2：データレジデンシーを持つ多国籍組織

各国政府は、さまざまな法規制を制定して、個人のデータプライバシー保護への関与を強めています。こうした保護は、組織の従業員、パートナー、顧客となりうる市民を対象とします。また、法規制の多くは国ごとに異なり、市民の個人識別情報（PII）について、多くの場合にそれぞれの国で保管することが求められます（データレジデンシー要件）。多国籍組織にとって、このように非常に複雑な規制環境でアイデンティティを管理・統制し、分散した多様な業務ユーザーにアプリケーションやサービスを提供することは大きな課題です。それが引き金となって、コンプライアンスの課題や生産性の低下が発生したり、サイロ化された環境全体で手作業による処理が必要になったりすることも珍しくありません。

Okta for Global 2000 を活用することで、ハブがさまざまなアプリケーションやプラットフォームサービスを提供できると同時に、適切な地域（スポーク）のみにユーザーの PII が永続的に保管されるようになり、従業員 / 顧客 / パートナーのデータレジデンシー要件に適合することが保証されます。

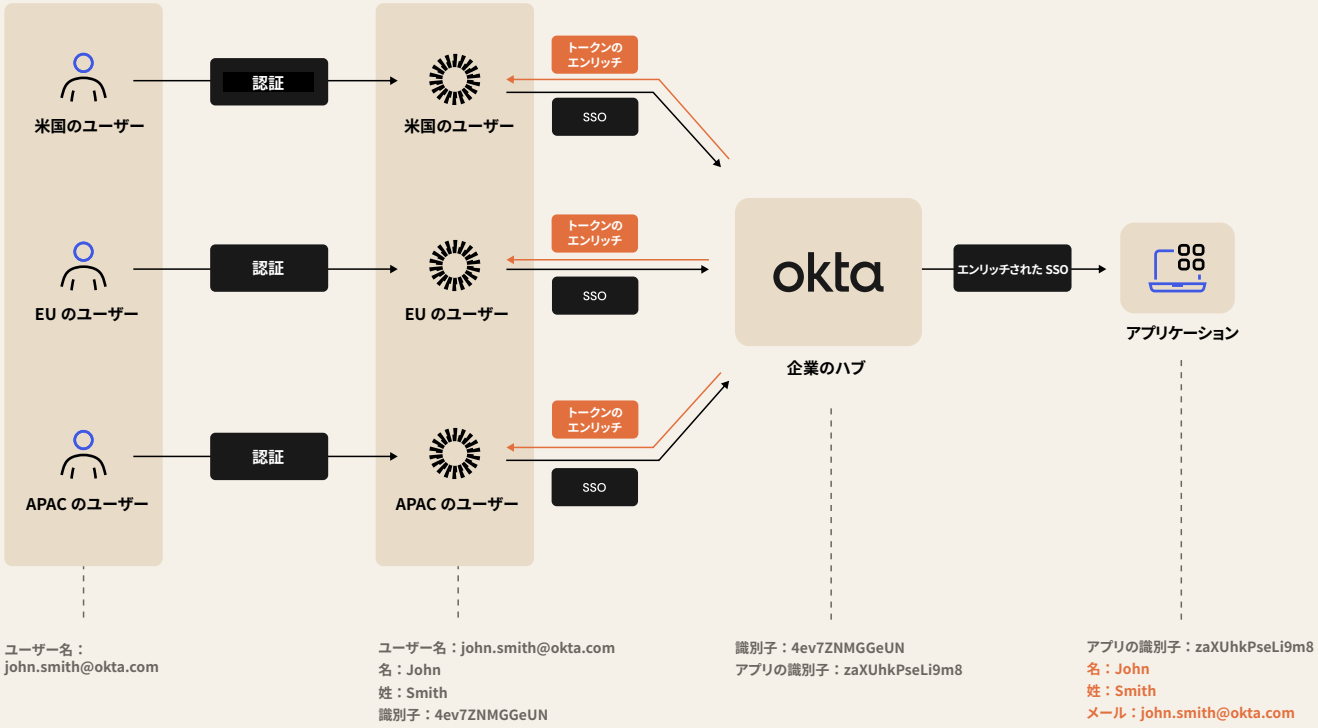
各地域（米国、EU、APAC）は、PII を含むユーザープロファイル情報を永続的に保存し、データレジデンシー要件を遵守するため、その地域内に独自のスポークを配置します。これらの地域スポークに保存されるユーザープロファイル情報は、スポーク内で直接作成された（Okta をソースとする）PII、またはユーザーのタイプに応じて他のリポジトリ（Active Directory、LDAP、HR アプリケーションなど）をソースとする PII を含みます。

プライバシーの維持

地域スポークは、PII を含むユーザープロファイル情報だけでなく、各ユーザープロファイルに固有の識別子も保存します。この一意の識別子は、PII を含まずに構築され、地域外で永続的なアイデンティティを作成する際や、ユーザーがアプリケーションにアクセスする際（SSO）の実行時に、参照可能なキーとして使用されます。この識別子を活用することで、ユーザーのプライバシーとデータレジデンシー要件の遵守の両方が確実に維持されます。さらに、ハブと統合された下流アプリケーションが実行時に PII を必要とする場合（SSO によるユーザーアクセス時）には、Okta Hooks の強力な能力をハブで利用し、スポークに保存された PII でアイデンティティトークンをエンリッチできます。エンリッチされたトークンは、下流のアプリケーションに渡されます。

Okta Hooks 機能を使用しても、PII がハブに永続的に保存されることはなく、PII は純粋に一時的なものであることに留意する必要があります。とはいえ、エンリッチによって PII を含むトークンの情報をアプリケーションが利用できるのは、実行時のユーザーセッション中に限定される必要があります。

プライバシーやデータレジデンシーの要件を満たすためには、アプリケーションが PII を永続的に保存（データベースストレージなどに）することは認められません。



展開モデル 2：データレジデンシーを持つ多国籍組織

展開モデル 3：サードパーティ（請負業者を含む）へのアウトソーシング

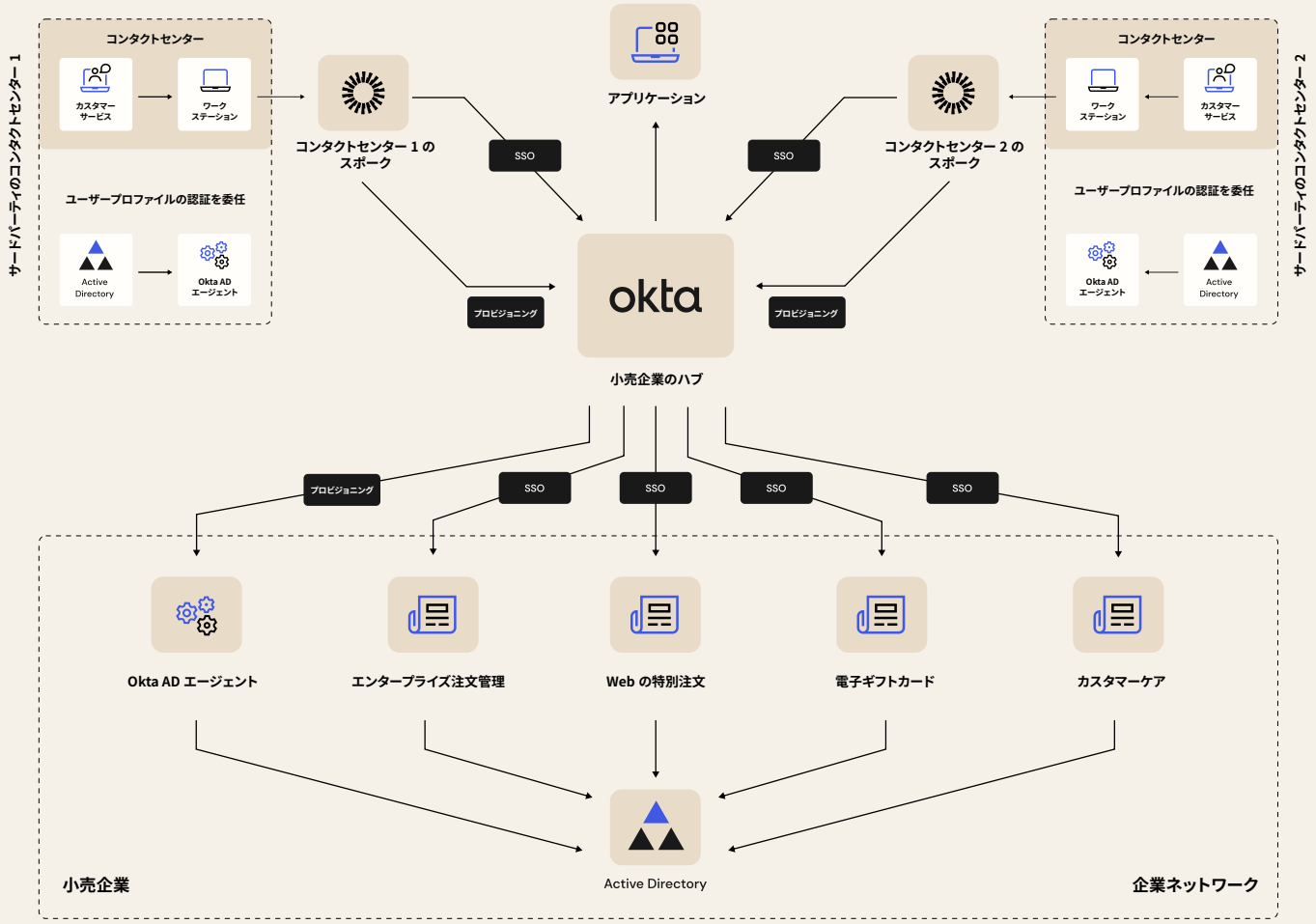
多くの組織は、効率性の向上、コストの削減、あるいは需要の急増（季節的な変動）に応じてビジネスを弾力的に拡張する場合など、さまざまな理由でコールセンターなどのビジネス機能をアウトソーシングしています。アプリケーションやサービスが、従来は従業員のみが使用するために設計されたものである場合、アウトソーシングした人材にもシームレスで安全なアクセスを提供しようとすると、テクノロジーとセキュリティの観点で新たな課題が生じる可能性があります。

Okta for Global 2000 を活用することで、企業（ハブ）は、オンプレミスとクラウドベースの両方で、さまざまなアプリケーションやプラットフォームサービスをアウトソーシングした人材に提供できます。

サードパーティのアウトソーシング組織は、それぞれが既存の Active Directory ユーザーリポジトリと Okta スポークを使用し、自社で管理するか、または自社の IdP をスポークにフェデレーションすることが可能です。サードパーティのアウトソーシング組織は、SSO とプロビジョニングの両面で、ハブが提供するアプリケーションやプラットフォームサービスに、シームレスかつ安全にアクセスできます。さらに、アウトソーシングされた人材は、引き続き Active Directory の既存の資格情報を使用して認証できます。最後に、ハブは必要に応じて、下流のアプリケーションやユーザーリポジトリへのユーザーアクセスのプロビジョニングを実行できます。

重要ポイントとしては、Active Directory での人員の管理をサードパーティのアウトソーシング組織に任せて、適切なアクセスを確保する一方で、Okta のグループとグループメンバーシップルールを使用して、アクセスに関係するハブ内で自社のセキュリティポリシーを適用できるというメリットがあります。Okta のサインオンポリシーによる多要素認証の使用も、必要に応じてハブを介して実装し、セキュリティレイヤーを追加できます。また、個人のアクセスを直ちに停止しなければならない場合には、サードパーティのアウトソーシング組織、その Active Directory、またはスポークからの支援を受けずに、ハブ内でユーザーアクセスを即座に停止 / 無効化できます。

最後に、アウトソーシングのパートナーシップが終了した場合、企業（ハブ）はスポークを切断し、そのスポークのユーザーのすべてのアクセスを即座に終了させることができます。



展開モデル 3：サードパーティ（請負業者を含む）へのアウトソーシング

Dick’s Sporting Goods の事例：季節性の要変動に合わせてシームレスに人員を増強

米国最大のスポーツ用品小売をオムニチャネルで展開している Dick's Sporting Goods は、外部の請負業者を通じて臨時の人員を調達しています。特に、冬のホリデーシーズン中は、顧客対応コールセンターを 4 つから 9 つに増やします。

このため、同社の IT チームは、新規のエージェント全員のオンボードを 1 か月未満で実行し、休暇明けにはその半分の期間でプロビジョニングを解除する必要があります。さらに、この手動オンボーディングを担うフルタイム従業員を 1.5 倍に増やさなければなりませんでした。したがって同社は、新しく業務に加わった人材に必要なツールを、より効率的かつ経済的に提供する方法を求めていました。

そのようなソリューションを提供したのが、Okta のハブアンドスポーク型アプローチです。BPO（ビジネスプロセスアウトソーシング）のパートナーは、それぞれに独自の Okta スポークを管理し、それが Dick’s Sporting Goods のハブに接続します。このアーキテクチャを使用して、同社のチームは、コールセンター、社内アプリケーション、注文管理、Web の特別注文、ギフトカードなどのプロビジョニングを実行します。BPO パートナーに対しても、運送業者やフルフィルメントパートナーなど、認証を必要とする外部アプリケーションへのアクセスを提供します。しかも、その際には複数の BPO で反復可能なプロセスを使用できます。

Okta を導入して以来、同社はライセンスコストを大幅に削減し、繁忙期の準備に必要な時間を短縮しました。

「Okta の統合が、当社のカスタマーサービス業務の価値を高めました。既存および新規の BPO パートナーは、アイデンティティの管理に責任を持ちます。この体制は、IT サポートとビジネスオペレーションチームの双方にとって画期的な変化をもたらしています。アウトソーシングされたエージェントは、当社のツールに簡単にアクセスでき、パスワードのリセットもセルフサービスで実行できるようになりました」

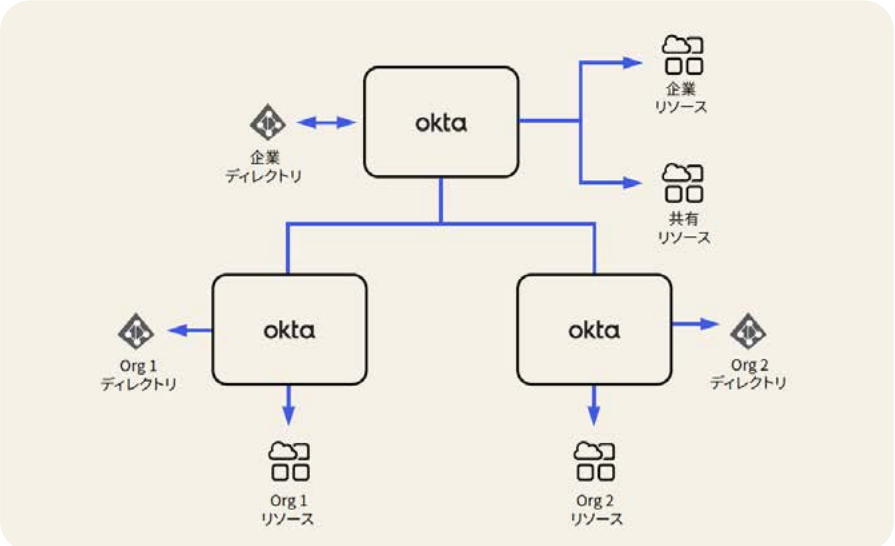
Eva Sciulli 氏
カスタマーインタラクション担当 IT プロダクトマネージャー
Dick's Sporting Goods

展開モデル 4：M&A 向けの統合

M&A はビジネスにとって重要な成長手段です。また、テクノロジーの円滑な統合は価値を加速させる上で不可欠です。アイデンティティは、M&A に伴うテクノロジーと人の変化の間で、共通レイヤーとしての役割を果たします。アイデンティティの「信頼できる唯一の情報源」を作成し、初日から重要アプリへのアクセスをユーザーに提供し、セキュリティポリシーを標準化することによって、M&A の統合の成果とスピードが高まります。

以下の図に示すアーキテクチャのように、Okta はあらゆるソースからのユーザーとグループの同期を可能にします。これにより、買収先の企業が Okta を使用している場合も、あるいは Active Directory、LDAP その他の IdP を使用している場合も、新しい従業員が初日から親会社の Okta org でアプリケーションに適切なレベルで容易にアクセスできるようになります。ハブアンドスポーク型アーキテクチャでは、こうしたユーザーは親会社の Okta org で管理されるようになるか、または買収先企業のディレクトリで管理された上で、親会社の Okta org との同期により共有リソースにアクセスできるようになります。

新しい従業員の生産性とセキュリティを高めるために、買収先企業に認証を委任することで、ログインでユーザー名やパスワードのリセットが不要のシームレスなユーザーエクスペリエンスを実現できます。それと同時に、ハブ内のアプリについては、親会社のセキュリティポリシーを適用できます。最後に、属性レベルのソーシングにより、親会社は個々のユーザー属性に異なるソースを指定できます。これにより、買収先企業のディレクトリの属性を上書きすることなく、共有アプリのプロビジョニングに必要な属性を制御できます。



組織に最適なハブアンドスポークの設計

Okta for Global 2000 は、独自のハブアンドスポーク型モデルを通じて、大規模組織に必要な柔軟性と分散型の自律性を提供しながら、組織全体でアイデンティティサービスを一元化します。これを活用することで、複雑なライフサイクル管理プロセスを簡素化して自動化する一方で、自社の従業員にとどまらない業務ユーザー全体にテクノロジーへのシームレスで安全なアクセスを提供できます。

組織の俊敏性を向上させるには、ユースケースに合わせてハブアンドスポークモデルを設計することが重要です。その方法、そして Okta for Global 2000 の詳細については、https://www.okta.com/products/global-2000/ をご覧ください。